Legislative Audit Division

State of Montana

Report to the Legislature

December 2003

Information System Audit

Statewide Accounting, Budgeting and Human Resource System (SABHRS)

Department of Administration

This report provides information regarding application controls over the state's enterprise computer system, and general controls over the related processing environment. It contains one recommendation to revisit the security planning process and update the SABHRS security plan.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

04DP-02

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb	Representative Dee Brown
Senator Mike Cooney	Representative Tim Callahan
Senator Jim Elliott, Vice Chair	Representative Hal Jacobson
Senator John Esp	Representative John Musgrove
Senator Dan Harrington	Representative Jeff Pattison, Chair
Senator Corey Stapleton	Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

December 2003

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our information system audit of controls relating to the state's central computer system operated by the Department of Administration. We performed a limited review of general and application controls over the Statewide Accounting, Budgeting and Human Resource System. This report contains one recommendation related to establishing a security planning process and implementing a security plan. The department's response to the audit report is contained at the end of the report.

We wish to express our appreciation to the department for their cooperation and assistance.

Respectfully submitted,

Signature on File

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Information System Audit

Statewide Accounting, Budgeting and Human Resource System (SABHRS)

Department of Administration

Members of the audit staff involved in this audit were Charles Nemec, David P. Nowacki, Ida L. Sajor, and Jessie Solem.

Table of Contents

Appointed and Administrative Officials

Department of Administration

Scott Darkenwald, Director

Cathy Muri, Administrator
Administrative Financial Services Division

John McEwen, Administrator
State Personnel Division

Brian Wolf, Chief Information Officer
Information Technology Services Division

Tony Herbert, Deputy Chief Information Officer
Information Technology Services Division

SABHRS Services Bureau

Chuck Virag, Bureau Chief

Nyla Johnson
Finance Lead

Jim Sheehy
Information Technology Lead

Theresa Scott
Budget Lead

Martha Watson
Human Resource Lead

Executive Summary

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is the state of Montana enterprise system for managing budget development, financial and human resource information. SABHRS is used by all state agencies to account for and report the use and disposition of all public money and property in accordance with state law. The state of Montana has just completed the fourth fiscal year using the SABHRS system.

SABHRS supports the core administrative processes used by all state agencies to account for and record financial and human resource data. The Legislative Audit Division, Information Systems audit team, examines selected SABHRS controls and operations each year. Our objectives are to provide reasonable assurance that controls exist to ensure data acquired from state agencies is properly processed and recorded, as well as appropriately secured from unauthorized or unnecessary access.

To meet our objectives, we conducted both general and application control testing. We evaluated the overall security of workstations, servers, databases, and network devices attached to, or used by, SABHRS to identify any potential security holes or risks. Tests were performed through the use of automated tools and review of setup files. We reviewed the procedures and policies in place at the SABHRS Services Bureau to determine that they are adequate for maintaining a minimum level of security.

Application controls operate only within the confines of the SABHRS applications. These controls guard the PeopleSoft application from inadvertent or intentional misuse and ensure that data are valid, properly authorized, completely and accurately processed, and available for use. Application controls are divided logically and physically into three separate domains: SABHRS Financials, SABHRS Human Resources Management System (HRMS) and the Montana Budget Analysis and Reporting System (MBARS). We did not include MBARS in our audit scope because MBARS is the system used to develop the budget, while the actual financial activity is accounted for on the SABHRS Financials

System. We evaluated whether access to data and system processing is controlled, whether processing is controlled to allow valid data to process while capturing invalid data, and whether additions or modifications to system processing are tested and controlled. We evaluated system tables, processing rules, and specific reports to determine whether tables contained correct data and reports containing processing results are reasonably constructed and tested to provide accurate information to users. The result of this work is the current audit report.

Conclusion

Based on our work, we conclude that controls exist to ensure data acquired from state agencies is properly processed and recorded for the processes tested. We conclude that security controls exist, but can be improved by management documenting its security considerations in a comprehensive, written security plan.

In addition to this report, we provide a limited distribution memorandum to Legislative Audit Division staff providing detailed internal control testing results and system and automated business process descriptions for SABHRS Finance and Human Resource application processes.

Chapter I – Introduction and Background

Introduction and Background

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is the state of Montana enterprise system for managing budget development, financial and human resource information. SABHRS is used by all state agencies to account for and report the use and disposition of all public money and property in accordance with state law. The state of Montana has just completed the fourth fiscal year using the SABHRS system.

Audit Objectives

SABHRS supports the core administrative processes used by all state agencies to account for and record financial and human resource data. Our objectives are to provide reasonable assurance that controls exist to ensure data acquired from state agencies (via on-line or electronic transmission) is properly processed and recorded, as well as, appropriately secured from unauthorized or unnecessary access.

The audit was conducted in accordance with Government Auditing Standards published by the United States General Accounting Office (GAO). We evaluated the control environment using state law and criteria established by the National Institute of Standards and Technology, Microsoft Best Practices for Enterprise Security, the Control Foundation's Control Objectives for Information and Technology, SANS Institute, and Carnegie Mellon.

Audit Scope and Methodology

General controls represent the baseline security of SABHRS while application controls are the application-level controls defined for each business process. General controls are an important barrier to prevent an individual from bypassing application controls and directly accessing or changing agency data. Poor general controls effectively nullify strong application controls, as it is possible to circumvent embedded Application Controls when one has direct access to the system resources.

To meet our objectives, we conducted both general and application control testing. We evaluated the overall security of workstations, servers, databases, and network devices attached to, or used by, SABHRS to identify any potential security holes or risks. Tests were performed through the use of automated tools and review of setup files. We reviewed the procedures and policies in place at the SABHRS Services Bureau to determine that they are adequate for maintaining a minimum level of security.

Application controls operate only within the confines of the SABHRS applications. These controls guard the PeopleSoft application from inadvertent or intentional misuse and ensure that data are valid, properly authorized, completely and accurately processed, and available for use. Application controls are divided logically and physically into three separate domains: SABHRS Financials, SABHRS Human Resources Management System (HRMS) and the Montana Budget Analysis and Reporting System (MBARS). We did not include MBARS in our audit scope because MBARS is the system used to develop the budget, while the actual financial activity is accounted for on the SABHRS Financials System. We evaluated whether access to data and system processing is controlled, whether processing is controlled to allow valid data to process while capturing invalid data, and whether additions or modifications to system processing are tested and controlled. We evaluated system tables, processing rules, and specific reports to determine whether tables contained correct data and reports containing processing results are reasonably constructed and tested to provide accurate information to users. The result of this work is the current audit report.

In addition to this report, we provide a limited distribution memorandum to Legislative Audit Division staff providing detailed internal control testing results and system and automated business process descriptions for SABHRS Finance and Human Resource application processes.

Conclusion

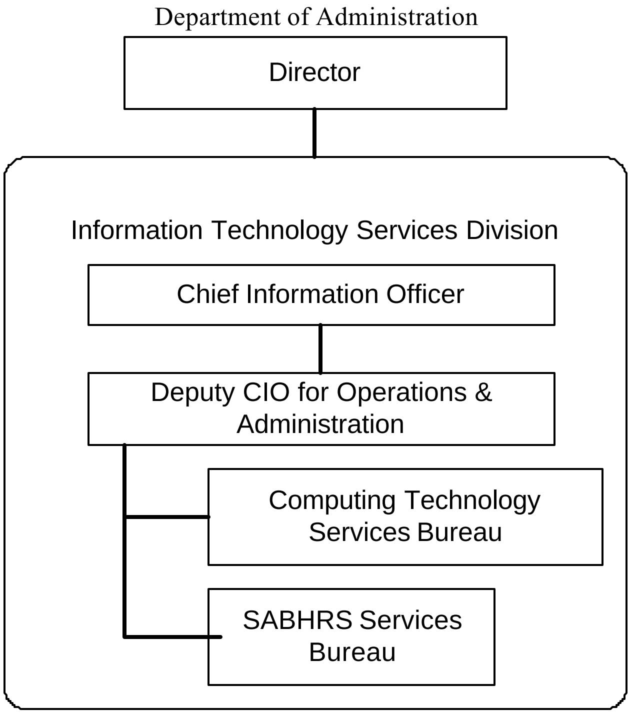
Based on our work, we conclude that controls exist to ensure data acquired from state agencies (via on-line or electronic transmission) is properly processed and recorded for the processes tested. We conclude that security controls exist, but can be improved by management documenting its security considerations in a comprehensive, written security plan.

Department of Administration Organizational Structure

State agencies are responsible for accurately entering their data into SABHRS. The Department of Administration is responsible for managing, operating and coordinating information technology and serving as the lead state agency for developing information technology and security. The department is also charged with establishing and enforcing statewide information technology policies and standards. Within the department, it is the Chief Information Officer and the Information and Technology Services Division (ITSD) that deliver information services, and oversee state information resources, policy and security.

SABHRS is one of the primary information services the department operates and the operation responsibility is assigned to SABHRS Services Bureau and the Computing Technology Services Bureau. The following chart shows the organization of SABHRS Services Bureau (SSB) and Computing and Technology Services Bureau (CTSB) within the Information Services Technology Division of the Department of Administration.

Figure 1


Department of Administration
Director
Information Technology Services Division
Chief Information Officer
Deputy CIO for Operations & Administration
Computing Technology Services Bureau
SABHRS Services Bureau

Source: Compiled by Legislative Audit Division.

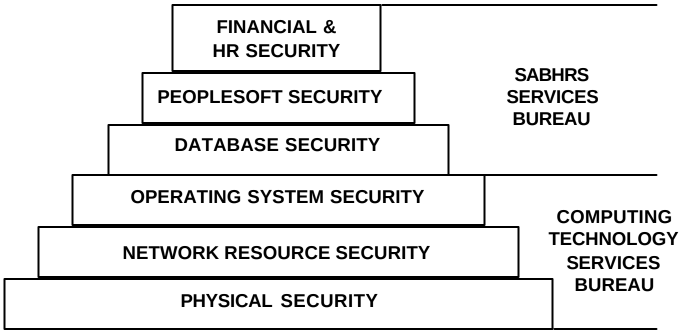
SABHRS Control Environment

SABHRS is a system existing as a collection of software, hardware, and communication connections each serving a purpose and operating together as the SABHRS operating environment. Ensuring this operating environment is secure is a coordinated responsibility of SSB and CTSB.

The following picture and accompanying descriptions depict the SABHRS Control Environment as a layer of security considerations and the associated bureau responsible for securing the layer. The Layered Security Concept means that the security of each layer is dependent on the security of the other layers. For example, SABHRS Financials and Human Resource (HR) applications security depend on the security of the five layers that support Financials and HR operations.

Figure 2

Layered View of SABHRS Control Environment



Source: Compiled by Legislative Audit Division

Physical Layer consists of network, database, and mainframe equipment location and surrounding environment. The layer includes secure physical access to equipment, location fire suppression, uninterruptible power supply to equipment, and location ventilation as examples.

Network Resources Layer is the connection entry point for agency personnel when accessing SABHRS. Agency personnel require use of the state's physical network, Internet and the state's Intranet, to connect to SABHRS.

Operating System Layer is composed of programs that manage information exchange between SABHRS and agency personal computers allowing the user to interact with or operate SABHRS.

Database Layer is where agencies' SABHRS data resides.

PeopleSoft Layer includes the programs that operate, manage, and configure SABHRS applications.

Financial and Human Resource Applications Layer is the final layer where users directly interact with SABHRS. This layer includes the programs that recognize and authenticates users allowing or restricting their actions, and programs that manage data, and organize, record, and report information.

Chapter II – Security

What is Security?

Security is a fundamental management responsibility, a duty to protect organization assets such as Montana's SABHRS system. Security in an electronic environment means anticipating dangers and reducing risks so the system survives and continues operating.

How is Security Managed?

The accepted method for managing security in an electronic environment is security planning, a process undertaken by management intended to protect systems. Planning is a process of considering and preparing for events that could disrupt system operations, cause data loss, or allow unauthorized data access, changes, or system use. Planning includes establishing ways to counteract or minimize the occurrence of those events. The tangible result of the planning process is a comprehensive, documented, dynamic security plan.

What is a Security Plan?

The National Institute of Standards and Technology's "Guide for Developing Security Plans for Information Systems" describes a security plan as a structured process documenting the system's value, threats or risks to the system, threat or risk vulnerability, matching safety measures and their effectiveness. A security plan should also be explicit, defining allowable behavior and responsibilities for all people accessing the system. Industry best practices suggest that a security planning process should begin by management examining the SABHRS environment:

- Identify and describe the SABHRS environment by asking:
  - What are SABHRS physical and logical assets?
  - What are critical functions?
  - What equipment houses or operates these functions?
- Identify risks or potential threats to SABHRS assets by asking:
  - What events can prevent SABHRS from doing its job?

  - What is the likelihood of these events happening?
  - What level of risk is management willing to accept to protect SABHRS?
- Determine presence of related vulnerabilities by asking:
  - Is SABHRS susceptible to the identified threat?
- Create safety measures to protect SABHRS assets by asking:
  - What precautions has management taken to reduce the risk to SABHRS?
- Assess safety measures effectiveness by asking:
  - How effective are precautions?
- Continuously evaluate and update the plan by asking:
  - What are new risks?
  - Is SABHRS vulnerable?
  - How should the plan change to counteract the new risk?

A security plan contains the answers to these questions along with assigning who is responsible and accountable for those answers. The following describes how we examined the SABHRS security environment, the examination results, and how the department responded to the results.

SABHRS Security Environment Examination

Most successful electronic attacks against information systems occur because attackers exploit well-known system weaknesses. These weaknesses, if not corrected or protected against, leave systems vulnerable. Section 2-15-114, MCA, requires agencies to include a general description of the existing security program and future plans for ensuring security of data in its agency information technology plans.

We requested the security plan for the SABHRS environment and evaluated it against suggested industry best practices.
Conclusion: We determined that the SABHRS security plan does not adequately describe the security environment.

We tested for common information system vulnerabilities in the SABHRS environment. Conclusion: The examination results indicated vulnerabilities are present, yet the SABHRS Security Plan does not specify whether management has considered these risks or address how management intends staff to manage them.
The following descriptions are the examination results and are organized to be consistent with the layered view of the SABHRS environment in Figure 2. Our testing was a controlled demonstration that vulnerabilities are present. Details of the identified vulnerabilities are not explicitly discussed but have been communicated to department management.

Physical Layer

The physical layer is both the SABHRS equipment location and location conditions. Potential events that pose a risk to the Physical Layer and can prevent SABHRS from accomplishing its tasks are fire, power interruption, malicious access, or environmental disaster. We examined ITSD location security, fire suppression, power supply and found the department is adequately addressing these risks through the ITSD disaster recovery planning process and environmental controls. ITSD is aware that a reliable, uninterruptible power supply is not available to fully operate or recover critical systems. ITSD staff are working to correct this deficiency.

Network Resources Layer

The network resources layer is the connection entry-point when accessing SABHRS. Users pass through the state's physical network, Internet and the state's Intranet, to connect to SABHRS. Network services are the "doors" and "windows" along the connection pathway and availability settings govern access through these "doors" and "windows." Network devices with inappropriate or unnecessary services available are a vulnerability and provide opportunities for a person or malicious program to gain system access to sensitive information, alter database content, compromise other network devices, and/or create damaging levels of network traffic. We examined selected Network Resource layer equipment services and availability settings and noted the following vulnerabilities are present and not addressed in the security plan.

We tested network devices for eight different services having commonly known vulnerabilities and discussed the following results with department staff:

1. *Information connection services available*: 10 of 17 devices had unnecessary connections available. Although these connections provide no information, they are an access point that provides a foot in the door to gain further entry to the system. These unnecessary connections are potential access "doors." Security best practices reduce the number of vulnerabilities by closing unnecessary connection "doors." Upon notification, department staff closed the connections. The SABHRS security plan does not identify this risk or include related safety measures.

2. *Information access services running*: 1of 2 devices tested provided an unnecessary ability to view system details that should not be accessible to just anyone. The unnecessary connection is a "window" that exposes the device's restricted information and vulnerabilities such as passwords, and configuration settings that could be used to gain further entry. Security best practices reduce the number of "windows" by closing unnecessary access. Upon notification, department staff closed the access. The SABHRS security plan does not identify this risk or include related safety measures.

3. *Information exchange services available*: 14 devices were tested and no unnecessary services were identified. However, the SABHRS security plan does not identify these devices, the required services necessary for their tasks, and any risks or related safety measures.

4. *Information access services running*: 3 of 6 devices tested identified services running without a business need. The unnecessary service provides a "door" that could allow unauthorized access to the device itself regardless if information is present or not. Security best practices reduce the number of "doors" by closing unnecessary access. Upon notification, department staff disabled unnecessary services for 3 devices.

The SABHRS security plan does not identify this risk or include related safety measures.

5. *Message services running*: 2 of 6 devices tested had message services running; however, the device is not intended for that purpose. A message service is an open "door" both to the device and other network users. Security best practices are to reduce the number of "doors" by closing this type of access. Upon notification, department staff closed the message services. The SABHRS security plan does not identify this risk or include related safety measures.

6. *Information exchange access available*: 2 of 7 devices tested provided an ability for anyone to connect without authenticating themselves by requiring a user name and password. This exchange procedure creates an open "door." Security best practices reduce the number of "doors" by closing this type of access if it is unnecessary or restricting its use to known users if it is necessary. Upon notification, department staff closed one device's unnecessary access and reconfigured the other device for greater security. The SABHRS security plan does not identify this risk or include related safety measures.

7. *Devices with unprotected access*: 5 of 5 devices tested were not password protected. While these are low-level service devices, their tasks can be interrupted or the device removed from service. Security best practices reduce this vulnerability by requiring password access thus restricting the device maintenance "door." Upon notification, department staff protected the devices with passwords. SABHRS security plan does not identify or discuss these devices, risks or related safety measures.

8. *Unrestricted connection access*: 7 of 7 devices tested had unrestricted connection access. This access is a "window" allowing information gathering that can be used to escalate access by using other vulnerabilities. Security best practices reduce this vulnerability by restricting access to other known devices or connections. Upon notification, department staff removed this vulnerability. The SABHRS security plan does not identify this risk or include related safety measures.

Operating System Layer

The operating system layer is composed of programs that manage information exchange between SABHRS and desktop computers allowing the user to interact with or operate SABHRS. Access vulnerabilities may be exploited so that a person can achieve unauthorized entry to a network or unauthorized access to data. We examined the Operating System layer and noted the following vulnerabilities are present and not addressed in the security plan.

We examined computer workstations for available communication connections and established unauthorized access with 31 workstations in the network segment tested. These workstations are possibly vulnerable to exploitation, however we did not attempt to exploit the vulnerability by accessing or changing information. We provided the test results to department staff. When notified, department management responded that the vulnerability is being removed from all identified workstations.

We noted two unknown accounts present on 1 network device. Although the accounts were disabled, the accounts could be activated and used to change how the device delivers information and interacts with other devices. Industry best practices state that unknown accounts should be removed instead of being inactivated. The SABHRS security plan does not identify this risk or include related safety measures. When notified, department staff responded the vulnerability would be closed because the device was being removed from service.

Database Layer

The database layer is where SABHRS data resides. Allowing staff to have direct access to database tables is a vulnerability. Direct access gives people the ability to create, alter, or destroy data or influence processing without leaving any trail to disclose these changes. In contrast to direct access, SABHRS users indirectly access data through the Finance or HRMS applications layer so that actions can be restricted and monitored.

We examined direct database access. Certain SSB staff have access to data and programs as a means of resolving processing problems or maintaining the database. This access and the actions they perform are not recorded or reviewed by other staff and accountability is not associated with single individuals having this access. These vulnerabilities are not adequately addressed in the SABHRS Security Plan. Department management contends that this access is necessary and there are no easy ways to monitor staff actions. However, the SABHRS database software does contain the ability to limit direct access and record staff actions for another person's review.

PeopleSoft Layer

The Peoplesoft layer includes the programs that operate, manage, and configure SABHRS applications. Peoplesoft program access can alter how SABHRS processes and records agency data as well as how SABHRS enforces financial transaction controls.

We examined SSB staff access and found staff had appropriate access. Also, we observed access controls operating that prevent unauthorized SABHRS users from accessing programs and functions. However, the SABHRS security plan contains high-level descriptions instead of specifying who is allowed access to these programs or the user responsibilities and expected behaviors.

Financial and Human Resource Applications Layer

The Financial and Human Resource Applications Layer includes the programs that recognize and authenticate users, allowing or restricting their actions based on their identity, and programs that manage data by accepting, organizing, recording, and reporting information. This is the final layer where users see and interact with SABHRS. Unauthorized access is a vulnerability that may exist when users' accounts remain active after personnel terminate employment or change jobs.

We identified thirteen former state employees and 2 former contract employees with active SABHRS access. This access was discontinued when auditors notified SABHRS and agency security staff. Continuing open access for individuals no longer authorized to have SABHRS access creates vulnerabilities that former employees, contractors, or other individuals with knowledge of this access may exploit. While written procedures exist instructing agency security officers to review agency staff access to SABHRS every three months, this process is not completely effective. In each of the past four SABHRS audits, we have identified unauthorized access as a continuing issue. Security planning should include periodic assessment of safety measures to determine their effectiveness or need for improvement. No periodic assessments are mentioned as part of the SABHRS Security Plan. Department staff rely exclusively on agency security officers for effective security performance.

Unauthorized access is also a vulnerability that may exist when users are given multiple types of access. Multiple accesses allow users to combine incompatible duties, effectively avoiding security measures designed to prevent inappropriate access to data and processes.

We identified six security access combinations that allow users to avoid intended security measures for certain transactions. We determined 13 of 334 SABHRS users having multiple access are assigned these incompatible combinations. Department staff depend on agency security officers to properly determine access including multiple accesses. However, we also noted one security officer with multiple accesses. SABHRS Services Bureau provides guidelines for agency security officers which states: " there are certain roles (accesses) which should not be mapped to the same user to insure a proper separation of duties. This is necessary to reduce the possibility of fraud or theft." No risk details, specific vulnerabilities or safety measures are discussed. Department staff have not considered including application access security measures in the SABHRS security plan since they have traditionally been considered separately as an agency security officer responsibility.

Summary

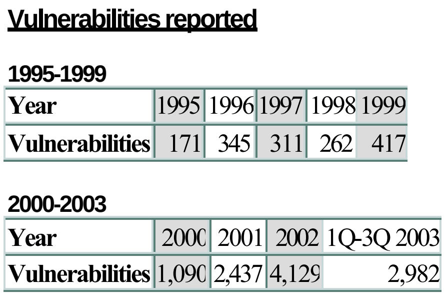
Examining the SABHRS security environment disclosed open vulnerabilities that may leave SABHRS susceptible to inadvertent misuse or malicious exploits. These vulnerabilities exist because the current SABHRS security-planning process is not comprehensive. Planning does not adequately consider risks and structure safety measures for the entire SABHRS environment.

Although SABHRS cannot be completely immune to attacks, following information industry security best practices will improve overall SABHRS security and make SABHRS less vulnerable. Security planning will identify key information and technology assets, critical failure points and risk mitigation tactics. A security plan is management's road map to an orderly and comprehensive security process and should direct staff on how to protect SABHRS. A security plan is cost-effective system protection concentrating limited resources on the most important information assets and focusing staff on management recognized vulnerabilities.

Finally, security planning should be a continuous process because vulnerabilities are constantly identified. A static plan will not protect SABHRS against each new risk. The following chart shows the number of vulnerabilities reported each year to CERT Coordination Center at Carnegie Mellon University and indicates the frequency that risks need to be considered.

Figure 3

Vulnerabilities Reported



Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	1Q-3Q 2003
Vulnerabilities	1,090	2,437	4,129	2,982

Source: CERT Coordination Center Carnegie Mellon University.

Recommendation #1

We recommend the department update the SABHRS security plan using a structured planning process that addresses:

- **Physical and logical assets**
- **Risks and potential threats**
- **Vulnerabilities present**
- **Safety measures and their effectiveness**
- **Continuous evaluation of new vulnerabilities**

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

JUDY MARTZ, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

November 26, 2003

Scott A. Seacat, Legislative Auditor
Legislative Audit Division
PO Box 201705
State Capitol
Helena, Montana 59620

Dear Mr. Seacat:

We have reviewed the November 2003 Statewide Accounting, Budgeting and Human Resource System (SABHRS) audit report and the recommendation contained therein. Our response to the recommendation follows.

Recommendation #1

We recommend the department revisit the SABHRS security plan using a structured planning process that addresses:

- Physical and logical assets
- Risks and potential threats
- Vulnerabilities present
- Safety measures and their effectiveness
- Continuous evaluation of new vulnerabilities

Response:

We concur. In the spring of 2003 we began taking steps to provide greater focus on the SABHRS security environment and plan. Portions of the security plan were modified and updated to meet some immediate needs. After this process, we completed the NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY Security Self-Assessment for Information Technology Systems for the SABHRS environment. Staff in the Information Technology Services Division (ITSD) Security Office evaluated the Self-Assessment response and developed related recommendations. These recommendations included additions to the current SABHRS Security Plan and/or the formulation of some additional written documentation such as policies and procedures. Further follow up related to these recommendations was delayed due to staff resource constraints resulting from the SABHRS Human Resources and Financials upgrade

"AN EQUAL OPPORTUNITY EMPLOYER"

projects. Staff in the ITSD Security Office will coordinate the development of updates to the SABHRS Security Plan or the creation of any additional documentation to include the recommended elements listed above, as well as any other additional recommendations resulting from the NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY Self-Assessment. Our goal is to accomplish these tasks by March 2004.

We thank you and your staff for conducting the audit in a professional manner.

Sincerely,

Scott Darkenwald

SCOTT DARKENWALD
Director